AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for re-encrypting encrypted data in a secure storage file system, comprising:

obtaining selected encrypted data from the secure storage file system using a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

decrypting the selected encrypted data using a first symmetric key to obtain selected data;

re-encrypting the selected data using a second symmetric key to obtain new encrypted data;

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing the new encrypted data and the new encrypted symmetric key if a second user ~~having~~ has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the private key to obtain encrypted hash data; and

storing [[an]] the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission.

2. (Previously Presented) The method of claim 1, wherein the user data access record comprises at least one selected from the group consisting of a bitmap for each user and a bitmap for each group of users.

3. (Original) The method of claim 1, wherein the write permission comprises at least one sub-division.

4. (Original) The method of claim 3, wherein the sub-division is selected from a group consisting of insert, append, truncate, and delete.

5. (Original) The method of claim 1, wherein the secure storage file system is implemented using a preloaded shared library.

6. (Original) The method of claim 5, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses.

7. (Original) The method of claim 1, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.

8. – 12 (Canceled)

13. (Currently Amended) A computer system generating a secure storage file system, comprising:

a processor;

a memory;

a storage device;

a computer display; and

software instructions stored in the memory for enabling the computer system under control of the processor, to perform:

obtaining selected encrypted data from the secure storage file system using a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

decrypting the selected encrypted data using a first symmetric key to obtain selected data;

re-encrypting the selected data using a second symmetric key to obtain new encrypted data;

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing the new encrypted data and the new encrypted symmetric key if a second user ~~having~~ has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the public key to obtain encrypted hash data; and

storing [[an]] the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission.

14. (Original) The computer system of claim 13, wherein the write permission comprises at least one sub-division.

15. (Previously Presented) The computer system of claim 14, wherein the sub-division is selected from a group consisting of insert, append, truncate, and delete.

16. (Original) The computer system of claim 13, wherein the secure storage file system is implemented using a preloaded shared library.

17. (Original) The computer system of claim 16, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses.

18. (Original) The computer system of claim 13, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.

19. (Previously Presented) The computer system of claim 13, wherein the user data access record comprises at least one selected from the group consisting of a bitmap for each user and a bitmap for each group of users.

20. (Currently Amended) A secure storage system comprising:

a storage provider storing encrypted data, wherein re-encrypting the encrypted data comprises:

obtaining selected encrypted data from the secure storage file system executing on the storage provider using a user data access record in response to receiving a key re-encryption event, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

decrypting the selected encrypted data using a first symmetric key to obtain selected data;

re-encrypting the selected data using a second symmetric key to obtain new encrypted data;

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing the new encrypted data and the new encrypted symmetric key if a second user ~~having~~ has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the private key to obtain encrypted hash data; and

storing [[an]] the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission; and

a client device, wherein the client device comprises a client kernel for generating the key re-encryption event and a client application using the encrypted data.

21. (Previously Presented) The system of claim 20, wherein the user data access record comprises at least one selected from the group consisting of a bitmap for each user and a bitmap for each group of users.

22. (Original) The system of claim 20, wherein the write permission comprises at least one sub-division.

23. (Original) The system of claim 22, wherein the sub-division is selected from a group consisting of append, truncate, and delete.

24. – 29 (Canceled)

30. (Previously Presented) An apparatus for re-encrypting encrypted data in a secure storage file system, comprising:

means for obtaining selected encrypted data from a secure storage file system using a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

means for decrypting the selected encrypted data using a first symmetric key to obtain selected data;

means for re-encrypting the selected data using a second symmetric key to obtain new encrypted data;

means for obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

means for encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

means for storing the new encrypted data and the new encrypted symmetric key if a second user ~~having~~ has read permission, wherein the second user is allowed access to the private key;

means for applying a hash function to the selected data to obtain hash data;

means for encrypting the hash data with the private key to obtain encrypted hash data; and

means for storing [[an]] the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission.